REMARKS/ARGUMENTS

Claims 1 to 33 are currently pending in the application. The Examiner has rejected claims 1, 2, 8-10, 12-16, 20 and 26 under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Patent No. 6,046,980 to Packer. Claim 17 has been rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Patent No. 6,144,636 to Aimoto et al. Claims 29-33 have been rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Patent No. 6,122,670 to Bennett. Claims 3- 5 have been rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Packer in view of Bennett. Claims 6 and 7 have been rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Packer in view of Aimoto. Claims 11, 27 and 28 have been rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Packer in view of Bennett. Claims 17-19 and 23-25 have been rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Aimoto in view of Bennett.

The Prior Art Rejections

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." See MPEP § 2131 (quoting *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

To support a rejection based on obviousness, the Examiner must, as the MPEP requires, articulate why a combination of references teaches or suggests all limitations of the claims. See MPEP §§ 2141, 2143. Furthermore, "'rejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.'" MPEP 2143.01, citing *KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, ___, 82 USPQ2d 1385, 1396 (2007), quoting *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006).

Claims 1, 20, 21 and 26

Claim 1 is directed to using behavioral models of network applications to classify network traffic. Claim 20 is directed to an apparatus that classifies data flows based on observed behavior, as well as explicitly-presented packet attributes. Claim 20 has been amended to further define application behavior model to include one or more of "a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows, an inter-packet timing value, a sequence of protocol flags, an inter-packet protocol flag timing value." Furthermore, claim 20 is directed to matching a data flow to a traffic class, if a threshold number of data flows of the host match a corresponding behavior model. Claim 21 is directed to an apparatus that classifies data flows based on observed behavior, as well as explicitly-presented packet attributes. Claim 21[1] has been previously amended to further define application behavior pattern to include one or more of "a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows, an inter-packet timing value, a sequence of protocol flags, or an inter-packet protocol flag timing value." Claim 26 has similar limitations to claims 20 and 21.

Packer fails to anticipate the subject matter of claims 1, 20, 21 and 26. Packer, like the prior art discussed in the background section of the present application, classifies network traffic based on inspection of explicitly presented attributes of packets in the data flows, such as protocol identifiers and the like. Claim 1, on the other hand, utilizes a knowledge base of known application behavior patterns to classify network traffic. The dependent claims, and the discussion that follows, present examples of application behavior patterns. As to claims 20, 21 and 26, Packer fails to disclose or suggest a system that classifies network traffic based on application behavior patterns and explicitly-presented packet attributes. Further, as to claims 20, 21 and 26, Packer fails to teach an application behavior pattern that includes one or more of "a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows, an inter-packet timing value, a sequence of protocol flags, or an inter-packet protocol flag timing value."

Still further, as to claim 20, nowhere does Packer teach the classification of a data flow based on the number of other data flows associated with a given host that also match a behavior

[1] The Office Action actually fails to explicitly define why claim 21 stands rejected. However, based on comments in the office action concerning certain dependent claims, Applicant assumes that the Examiner has rejected claim 21 based on Packer.

pattern.

Claims 2-5

Claims 2 to 5 are directed to the classification of data flows based on a behavior pattern that considers the sizes of packets.

As to claim 2, the Examiner alleges that Packer teaches classification of a data flow based on the packet size of a packet in the data flow. This allegation is plainly unsupportable. For example, the Examiner points to Table 2 of Packer (Col. 12). Table 2 of Packer merely depicts some of the attributes that may be used to classify network traffic. None of these attributes, however, are directed to the size of the packets of a data flow. Indeed, Packer is devoid of any teaching that discloses or suggests consideration of packet size or patterns that include packet size in the classification of data flows.

The Examiner appears to allege that the combination of Bennett and Packer teaches the subject matter of claims 3 to 5. Again, this contention is unsupportable. The Examiner's reliance of the fragmentation processes disclosed in Bennett is completely misplaced. Bennett appears to describe a system that offloads reliable communications protocol processing (such as TCP) to hardware. Bennett, Col. 1, line 57 to Col. 2, line 9; Col. 3, lines 46-57. Indeed, the teachings in Bennett, on which the Examiner relies, are directed to receiving a packet and computing a checksum as a lookup to identify other packets that may have been accumulated according to a defragmentation process. Nothing in Bennett, however, teaches classification of data flows into "network application traffic classifications" based on behavior patterns that consider the sizes of packets of a data flow.

Still further, the amendments to claim 1 further distinguish the claimed subject matter from Packer and Bennett. As discussed above, the Examiner relies on the teachings of Bennett to allege that examination of packet size of a first packet in the data flow is used to classify traffic. Bennett merely identifies whether received ATM cells are IP packet fragments in order to facilitate packet re-assembly operations. The flag and offset mentioned in Bennett allow for identification of the datagram fragments. However, neither Packer nor Bennett disclose classifying a data flow "into a network application classification" based on a comparison between an application behavior pattern corresponding to the network application classification and any attributes associated with fragment identifiers taught in Bennett.

Claims 6 and 7

Claims 6 and 7 are directed to a traffic classification system that uses a behavior pattern that considers the information density of respective packets. Claims 6 and 7 have been amended to state that "information density corresponds to a level of randomness of data of the at least one packet."

The Examiner appears to allege that Aimoto, in combination with Packer, renders obvious the subject matter of claims 6 and 7. Again, the Examiner's reliance on Aimoto is completely misplaced. Aimoto merely describes a packet switching function that addresses network congestion. The passage of Aimoto cited by the Examiner teaches the use of a packet buffer shared by a plurality of output ports. For each traffic class, a counter is maintained. A congestion notification is generated when a threshold cell count number is exceeded. Aimoto, Col. 3, lines 7-22. The Examiner appears to allege that a threshold relating to the number of cells buffered for a given traffic class is equivalent to the "information density" of a packet. Information density is disclosed at paragraph 0051 of Applicant's specification. Information density characterizes the level of randomness in the data of a given packet. Accordingly, the Examiner appears to incorrectly equate a congestion threshold based on the number of packets stored in a buffer with a metric that characterizes the density of information of a packet. Still further, the Examiner's rejection is also improper because the Examiner fails to consider that, even assuming Aimoto teaches the concept of information density, Aimoto does not teach the use of information density to classify data flows.

Claims 8 and 9

Claims 8 and 9 are directed to a traffic classification system that uses a behavior pattern that considers the presence of other, similar data flows associated with the same host. Claim 8 involves an evaluation of the timing of these related flows, while claim 9 involves evaluation of the number of related flows. Paragraphs 0052 and 0053 of the specification teach this subject matter.

The Examiner incorrectly alleges that Packer discloses the subject matter of claims 8 and 9. The passage of Packer (Col. 10, lines 32-42) merely discloses the detection of a data rate based on the timing of when a packets of a single data flow are received. Accordingly, the Examiner's rejection is incorrect for two reasons. First, Packer does not disclose consideration of the timing or number of related or similar flows associated with a host. Second, Packer fails to disclose consideration of the timing or number of related or similar data flows associated with a host for the purposes of classifying a data flow.

Claims 10 to 16

Claims 10 to 16 are directed to a traffic classification system that uses a behavior pattern that considers the timing of various events associated with a data flow, such as the timing between two packets of a flow, the timing and sequence of protocol flags and the like.

As to claims 10 to 16, the Examiner's reliance on Packer is fatally defective. The common error across the Examiner's rejections is the recital of some disclosed function in Packer, such as examination of data rate, without any support in Packer that the recited function is used in a behavior pattern against which data flows may be classified. Furthermore, as to claim 10, while Packer discloses identification of a data rate, it does not disclose use of a data rate to classify network traffic.

As to claim 11, the rejection is improper as the rejection fails to actually apply the teachings of Bennett to the claim language. Specifically, the Office Action fails to identify how Bennett teaches the inspection of a sequence of protocol flags of a data flow is used to classify network traffic into a network application traffic classification.

Claim 17

Claims 17 to 19 are directed to methods that model the behavior of a network application and using the modeled behavior to classify network traffic. The application behavior pattern includes at least one instance of a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows. Claim 17 has also been amended to state that the application behavior pattern corresponds to the network application, and to include "configuring a network traffic monitoring device to monitor data flows relative to at least one behavioral attribute and classify the data flows into a traffic class of a plurality of traffic classes by comparing one or more of the data flows against the application behavior pattern."

The Examiner's reliance on Aimoto to reject claim 17 is misplaced . Aimoto is directed to a network switch with a congestion control function. The metrics monitored by Aimoto such as cell count, bit rate, and the like are monitored relative to respective traffic classes. Aimoto, however, does not use such metrics to actually classify the network traffic. Rather, Aimoto uses the standard paradigm to classify network traffic. That is, the network switch of Aimoto uses explicitly presented attributes of the cells (here, Switched of Permanent Virtual Connection identifiers—termed "VCIs" in Aimoto) to associate the cells with a traffic class. The metrics maintained by Aimoto are used to control congestion, not classify traffic.

Claims 29 to 32

Independent claim 29 has been amended to clarify that computed entropy values are used to classify data flows. Claim 29 has also been amended to define entropy information as a "level of randomness of data of the at least one packet."

As discussed above, neither Bennett nor Aimoto, disclose the classification of network traffic based on entropy or information density of packets of a data flow. Aimoto has been discussed above in connection with claims 6 and 7. Bennett merely computes checksums of IP addresses or other headers to match packets that have been buffered as part of a defragmentation process. As discussed, Bennett does not teach the application of an entropy or information density function to classify data flows.

Claim 33

Lastly, claim 33 was previously amended to clarify that the received packets of a data flow have respective first checksums, and that classification is based on computing second checksums and comparing the second checksums to the first checksums contained in the packets.

The Examiner's reliance of the fragmentation processes disclosed in Bennett is again misplaced. The quoted passages of Bennett teach receiving a packet and computing a checksum as a lookup to identify other packets that may have been accumulated according to a defragmentation process. Matching packets to a data flow taught in Bennett does not teach or suggest classification of the data flows themselves. Nothing in Bennett, however, teaches classification of data flows based on behavior patterns that consider whether the computed second checksum should match the checksum contained in received packets. Indeed, checksums are generally used to check for transmission errors. The claimed subject matter is a novel use of checksums to classify network traffic based on the existence of some network applications that intentionally include incorrect checksums. See Specification at ¶ 0056.

CONCLUSION

In light of the foregoing, Applicants believe that all currently pending claims are presently in condition for allowance. Applicants respectfully request a timely Notice of Allowance be issued in this case.

If a telephone conference would advance prosecution of this Application, the Examiner may call Mark J. Spolyar, Attorney for Applicant, at 650-739-7511.

The Commissioner is hereby authorized to charge $490.00 for response within second month under 37 C.F.R. §1.136(a) fee set forth in 37 C.F.R. §1.17(a)(2) and any fee and credit any overpayment to Deposit Account No. 02-0384 of Baker Botts LLP.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant

Mark Spolyar

Mark J. Spolyar

Reg. No. 42,164

Date: October 15, 2008

Correspondence Address:
Customer Number: **05073**